DO YOU KNOW?

YOUR BODY, YOUR DATA, YOUR RULES — HERE'S WHAT THE DPDP ACT MEANS FOR YOU.

Biometric Data & the DPDP Act — How India's new privacy law protects (and limits) your most personal information.

WHAT COUNTS AS BIOMETRIC DATA?

- Biometric data = any personal data derived from physical, physiological, or behavioural traits used to identify an individual.

- Includes: fingerprints, iris scans, facial recognition data, voice patterns, gait, and keystroke dynamics.

- It’s immutable — *once stolen, you can’t “reset”* it like a password.

WHY IT MATTERS

- Biometric data enables convenience—unlock phones, verify payments, board flights.
- But it also poses unique privacy risks:
  - Permanent identity theft
  - Mass surveillance potential
  - Function creep (use beyond original purpose)

DPDP ACT: WHAT THE LAW SAYS?

- Defines “personal data” broadly includes biometric identifiers.
- Requires free, specific, informed consent before processing any personal data.
- Allows processing of sensitive data (like biometrics) only when necessary and with clear purpose limitation.

SENSITIVE DATA, SIMPLIFIED

- While the DPDP Act does not explicitly label “sensitive personal data,” its intent and structure mirror earlier drafts (e.g., PDP Bill, 2019).
- Biometrics are treated as high-risk data under governance and consent requirements.
- Key idea: The more personal the data, the higher the consent threshold.

THE CONSENT PRINCIPLE

- ✅ Must be informed, specific, and revocable.
- ❌ Blanket consent or pre-ticked boxes = invalid.
- 💡 Data Fiduciaries must give users clear notice before collection; in plain language, including how long data will be retained.

FOR TECH COMPANIES: COMPLIANCE CHECKLIST

- Conduct Data Protection Impact Assessments (DPIAs) for biometric processing.
- Implement privacy-by-design architecture.
- Store biometric templates securely — prefer on-device processing where possible.
- Enable consent dashboards for users to withdraw or review data.

THE GLOBAL LENS

- GDPR (EU): Classifies biometrics as special category data (Art. 9).
- U.S. States (Illinois, Texas): Biometric-specific laws with strict consent & retention limits.
- India: DPDP builds a foundational layer — enforcement & rules will define its real strength.

CRGCL INSIGHT

- CRGCL recommends:
  - Establishing biometric-specific rules under DPDP.
  - Stronger anonymisation standards & purpose audits.
  - Awareness drives for consent literacy among users.

Centre for Research and
Governance on Cyber Law

Empower Yourself—
Know Your Digital Rights!

Share this post to spread awareness.
Follow CRGCL for more updates on digital governance and cyber law.

www.crgcl.com